17 January 2018

Comments by the Centre for Information Policy Leadership

on the Article 29 Data Protection Working Party's

Working Documents Setting Up Tables for Binding Corporate Rules and Processor Binding Corporate Rules

adopted on 29 November 2017

On 29 November 2017, the Article 29 Data Protection Working Party ("WP29") adopted two updated Working Documents setting up a table with the elements and principles to be found in Binding Corporate Rules ("WP256") and Processor Binding Corporate Rules ("WP257") (collectively the "Working Documents"). The WP29 invited public comments on these documents by 17 January 2018. The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to submit the comments below.

Binding Corporate Rules (BCR), a voluntary scheme whereby a corporate group commits to a binding set of enhanced data protection requirements across their group, serve not only as a data transfer tool but also as an internal privacy compliance program and accountability tool. Adopting and implementing BCR is by no means a trivial process and companies that choose to seek approval are undertaking a serious commitment that requires considerable financial investment and resources.

The requirements for BCR were originally set forth by the WP29 in previous editions to the Working Documents.[2]

Article 47 of the GDPR incorporates BCR into legislation for the first time. The updated WP29 Working Documents seek to incorporate the new elements of BCR as outlined under the GDPR.

De facto, BCR go beyond being a data transfer mechanism. BCR are viewed as a certification[3] for a company's privacy management and compliance program and act as a

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton & Williams LLP and is financially supported by the law firm and 59 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton & Williams.

[2] WP153 Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp153_en.pdf; and WP195 Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf.

[3] Previous CIPL work recommends that BCR should be leveraged and "upgraded" to GDPR certification under Articles 42 and 43. See https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf at page 11-12. Although it is currently unclear whether certification or seals will be

"badge of recognition" by data protection authorities (DPAs). Since its introduction in 2003,[4] over 105 multinational companies have successfully implemented BCR.[5] While the mechanism seems to be gaining popularity, it is still perceived as a gold-plate approach, suitable for large organisations with significant resources, a dedicated data protection officer (DPO) and large teams. To facilitate their wider use, that is not limited to only the largest organisations, BCR need to be made scalable and configurable to the needs of organisations of all sizes and corporate structures. This is especially important given that more organisations may adopt BCR as their preferred transfer mechanism in the future (as supported by the results of the CIPL and AvePoint GDPR Readiness Survey[6] 2016 and 2017).

The key challenge is rooted in the need for approval of BCR by a DPA and a slow review and approval process that also varies by DPA depending on their experience and workload. Given this lengthy and rigorous process, the WP29 should revise and streamline the Working Documents to ensure that BCR become user friendly and straightforward documents that do not unnecessarily repeat requirements that are clearly outlined by the GDPR.

Comments

Comments Applicable to Both Controller and Processor BCR (BCR-C and BCR-P)

1. BCR Scope of Application

See "New Elements" Section in WP256 (p. 3) and WP257 (p. 3)

Under the "New Elements" section of both Working Documents, the WP29 restates the requirement of Article 47(2)(a) GDPR that the BCR shall specify the structure and contact details of the group of undertakings or group of enterprises engaged in a joint economic activity and of each of its members. CIPL suggests that the WP29 remain flexible on how these contact details can be provided, to ensure they remain accessible, useful and viable for individuals and regulators. For example, in a large multinational company, a single point of contact, such as a DPO or a member of a DPO team, for all the entities may be more helpful, both for individuals and regulators. This also aligns with the requirement of the GDPR to provide contact details of the DPO to the DPAs and the public. BCR-approved companies may discharge this obligation under the GDPR and BCR in the same instance.

---

provided for program-level compliance versus specific processing-level compliance, CIPL believes that BCR presently and in the future should define the baseline standards for the demonstration of program-level accountability and compliance.

[4] WP74 Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp74_en.pdf.

[5] List of companies for which the EU BCR cooperation procedure is closed http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48705.

[6] See the first edition of CIPL and AvePoint's Report on Organisational Readiness for the European Union General Data Protection Regulation, detailing the 2016 survey results https://www.informationpolicycentre.com/global-readiness-benchmarks-for-gdpr.html. At the time of writing, the second edition of the report detailing the 2017 survey results is pending release.

<u>Recommendation</u>: Clarify that specifying the contact details of the group members as required by Article 47(2)(a) can be achieved by providing the contact information of a single point of contact within a company, such as a DPO or a member of a DPO team.

2. <u>Creation of Third-Party Beneficiary Rights for Individuals</u>

See Section 1.3 of Tables in WP256 (p. 6-8) and WP257 (p. 5-8)

2.1. The Working Documents note in Section 1.3 that individuals must be able to enforce the failure of a company to abide by the duty to be transparent when national legislation prevents compliance with BCR. Section 1.3 refers to the obligation of the company to notify the Supervisory Authority pursuant to Article 47(2)(m) of the GDPR and cross references to Section 6.3 of the Working Documents. CIPL questions the practicality of this requirement given that the individual would not even be aware of whether a company has notified the Supervisory Authority. Furthermore, in respect of BCR-P and processors, it would be even less likely that an individual would know of every single processor (especially when an individual has a primary relationship with a controller) and be able to challenge the processor's obligation to notify the controller or a competent Supervisory Authority. Therefore, CIPL believes the WP29 should delete this point from Section 1.3 of the Working Documents.

<u>Recommendation</u>: Clarify that enforcing the obligation outlined in Section 6.3 of the Working Documents (obligation to notify the Supervisory Authority when national legislation may prevent respect of BCR) is the prerogative of the Supervisory Authority itself and not an enforceable right of an individual.

2.2. The Working Documents further note in Section 1.3 that individuals must be able to enforce the duty to cooperate with the DPA. CIPL believes the WP29 should remove this element from the Working Documents because a duty to cooperate with the DPA is an obligation of the BCR company in relation to the Supervisory Authority. Section 3.1 of the Working Documents on the duty to cooperate with Supervisory Authorities notes that the BCR should contain a clear duty for all BCR members to cooperate with and to accept to be audited by the Supervisory Authorities and to comply with the advice of these Supervisory Authorities on any issue related to those rules. It is both impractical and difficult to imagine how such a duty can be enforced by an individual, as a third-party beneficiary.

<u>Recommendation</u>: Remove the duty to cooperate with the DPA as an element of BCR enforceable by third-party beneficiaries.

3. <u>Requirement That the Company Has Sufficient Assets</u>

See Section 1.5 of Table in WP256 (p. 9) and Section 1.6 of Table in WP257 (p. 9)

The Working Documents note that the application form must contain confirmation that any BCR member in the EU accepting liability for the acts of other BCR members (and/or any external sub-processors in the case of BCR-P) bound by the BCR outside of the EU has

sufficient assets to pay compensation for damages resulting from a breach of the BCR. The WP29 should clarify that the duty to pay for damages does not extend to responsibility for fines imposed by DPAs under the GDPR and is limited to actual demonstrable damages which may be recovered under the GDPR. A European affiliate alone often would not possibly be able to provide confirmation of sufficient assets to cover the level of fines introduced in the GDPR (i.e. up to 4% of annual worldwide turnover of the entire BCR entity in this case). Additionally, a guarantee from the parent company should be sufficient confirmation of assets to pay compensation for damages as such a guarantee is generally accepted under current BCR practice. Indeed, based on the accepted accounting principles within corporate groups, it is irrelevant which particular entity "pays the bill", as the financial impact will be felt and reflected at group level (in global revenue, profit and share price). Therefore, CIPL believes that in light of the possibility of damages claims under the GDPR this requirement of the WP29 (which already exists under the current BCR regime and previous editions of the Working Documents[7]) should be updated to allow the liable company to demonstrate that it has "access to sufficient assets" to cover damages under the GDPR. In this way, even if a single EU entity cannot alone bear the financial impact of a BCR breach, they may resort to using corporate group funds and cover the cost of a violation centrally. For individuals and DPAs, it should be irrelevant where the money comes from, as long as the liable entity is able to pay the damages.

Recommendation: Clarify that the requirement of BCR members to provide confirmation of sufficient assets to pay for damages resulting from a breach of the BCR by members outside the EU does not extend to responsibility for fines imposed under the GDPR and is limited to actual demonstrable damages which may be recovered under the GDPR. In addition, update the Working Documents to specify that the liable company must only provide confirmation of access to sufficient assets to cover any such damages and that a guarantee from the parent company is one way of demonstrating such access.

4. Description of the Material Scope of the BCR

See Section 4.1 of Tables in WP256 (p. 14) and WP257 (p. 14)

One element the Working Documents state for specifying the material scope of the BCR is the identification of recipients in a third country[8] or countries (in WP256) and data importers/exporters in the EU and outside the EU (in WP257). Article 47(2)(b) of the GDPR only requires that the third country or countries be identified. There is no mention of identifying the actual recipients or actual data importers/exporters. This requirement does not appear in the previous versions of the Working Documents[9] either. Requiring the identification of every single actual recipient or data importer/exporter presents an additional and excessive burden on companies, especially as processing arrangements often change. CIPL recommends that the working party delete this requirement and use the

[7] See Footnote 2.
[8] For consistency with its previous guidance documents, the WP29 should clarify that a "third country" refers to any non-EEA country.
[9] See Footnote 2 and BCR Standard Application Form WP133 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp133_en.doc.

wording provided by Article 47(2)(b) of the GDPR which requires that only the country itself be identified. In any case, BCR do not need to specify all the recipients in a corporate group, or data importers/exporters, as that information is listed as part of the BCR application and kept by the BCR-approved company.

Recommendation: Delete the requirement that the identity of actual recipients of data or importers and exporters of data in third countries be identified in the BCR and replace it with the wording used in Article 47(2)(b) of the GDPR which requires only the country itself be identified.

5. Process for Updating the BCR

See Section 5.1 of Tables in WP256 (p. 15) and WP257 (p. 14)

5.1. The Working Documents note that any changes to the BCR or to the list of BCR members should be reported once a year to the competent Supervisory Authority with a brief explanation of the reasons justifying the update. The WP29 should confirm that updating the BCR to be in line with the GDPR falls under this reporting procedure and BCR companies should send their updated version of the BCR to the Supervisory Authority.

Recommendation: Confirm that companies seeking to bring their BCR in line with the GDPR must update them in line with the requirements of WP256 and WP257 and send the updated BCR to the competent Supervisory Authority.

5.2. The Working Documents further note that updates to the BCR or list of members of the BCR are possible without having to reapply for approval provided that "[a]n identified person keeps a fully updated list of the BCR members and keeps track of and record[s] any updates to the rules…" CIPL recommends that the WP29 remains flexible on this requirement and clarifies that an identified person responsible for keeping track of updates could be a specified individual or identified team within an organisation and does not necessarily have to be a DPO or member of a DPO team but can be someone from another department such as corporate and legal affairs, taxation or entity matters, etc.

Recommendation: Clarify that an identified person responsible for noting updates to the BCR can be an individual or a responsible team across the corporation with discretion left to companies to determine who or which team is best suited for the task.

5.3. In order to ensure clarity and consistency, for both DPAs and companies, the WP29 may want to recommend that organisations with existing BCR add an introductory statement to their updated BCR acknowledging that they were approved prior to the GDPR and have now been updated in accordance with the requirements. Additionally, such a statement could serve as confirmation that companies have updated the content of the BCR to meet the requirements of the GDPR and the Working Documents but have not made any changes that would constitute a significant or material change to the binding nature of the BCR.

<u>Recommendation</u>: Suggest that companies include in their updated BCR an introductory statement acknowledging that the document has been updated in line with the GDPR and the Working Documents and that changes to content reflect these updates but do not constitute a significant or material change to the binding nature of the BCR.

5.4. In addition, some companies are and will still be in the process of approval of their BCR through a national mutual recognition procedure come May 2018 (i.e. they have obtained BCR approval from the lead DPA, but are still going through individual Member State national procedures). It is unclear from the Working Documents what the transitional arrangements should be for these companies. To streamline the process and not create further delays, CIPL recommends that these BCR should be treated the same as fully approved BCR, given that the mutual recognition process and Member State approvals will be eliminated under the GDPR, and these companies can simply update their BCR in line with the GDPR and send the changes to the competent Supervisory Authority.

<u>Recommendation</u>: Clarify that companies still in the process of approval of their BCR through a national mutual recognition procedure should be treated the same as fully approved BCR and must simply update their BCR in line with the requirements of the GDPR and send the updated version to the competent Supervisory Authority.

Comments Applicable to Controller BCR Only (BCR-C)

This section of comments concerns WP256 only.

1. <u>Requirement to Sign a Contract Comprising the Requirements of Article 28(3) GDPR</u>

See "Introduction" Section in WP256 (p. 2)

The introduction to WP256 refers to the requirement in Article 28(3) of the GDPR that a contract or another legal act under Union/Member State law, binding on the processor with regard to the controller and which comprise all the requirements as set out in Article 28(3) GDPR should be signed with all internal and external subcontractors/processors. WP256 refers to such a contract as the Service Agreement.

We recommend that the WP29 clarify that companies with approved BCR-C do not have to implement additional controller-processor contracts reiterating the processors' obligations under Article 28(3) GDPR in respect of internal transfers between controllers and processors within the same group of companies. This recommendation is based on the fact that:

a. **BCR already incorporate the requirements of Article 28 GDPR:** BCR, updated and brought into line with the GDPR embed the requirements of Article 28 (for example, the instructions to internal processors to act on behalf of internal controllers, the obligation of confidentiality for persons authorised to process personal data, the obligations to apply appropriate security measures, to respect data subject rights, to

perform a data protection impact assessment (DPIA) under certain circumstances, to delete personal data once the processing has concluded, etc.);

b. **BCR-C must be made binding on all participating group members:** Section 1.2 of the criteria for approval of BCR in WP256 notes that the group will have to explain in its BCR application form how the rules are made binding for each participating company/entity in the group (either by intra-group agreement, unilateral undertakings or by other means chosen by the company). Such a binding mechanism results, by definition, in each group member committing to process personal data in accordance with the requirements of the GDPR and BCR, which both include the Article 28 requirements. Therefore, asking group members to execute in addition to the BCR binding mechanism/intra-group agreement, separate Article 28(3) agreements for multiple data transfers between multiple internal controllers and processors presents no additional value and just creates additional administrative barriers for the BCR-approved company. Indeed, simplifying and streamlining mechanisms for internal data transfers within a multinational company were the "raison d'être" of the BCR;

c. **The BCR binding mechanism/agreement coupled with the Article 30 records of processing requirements cover the requirements of Article 28(3):** Article 28(3) requires that a controller-processor contract set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. As this information is specific to each processing and keeps on changing with new processing and new transfers within the group, it cannot be included in advance in BCR, or in the binding mechanism. However, the binding nature of BCR, updated in line with the GDPR, along with the requirement to maintain a record of data processing activities under Article 30 GDPR and the existence of internal operational policies and instructions between various entities processing data, makes the requirement for an additional Article 28(3) contract unnecessary; and

d. **This new suggestion by the WP29 is contrary to existing practice with approved BCR-C:** The WP29's suggestion that companies with approved BCR-C implement additional controller-processor contracts under the circumstances outlined above has not been required to date and is contrary to existing practice with respect to approved BCR-C.

<u>Recommendation</u>: Clarify that, because BCR-C, updated and brought into line with the GDPR, already embed the requirements of Article 28, there is no need to execute any additional contracts between the internal controller and internal processor entities. Rather, the Working Documents should only reiterate that the provisions found in Article 28 must be an integral part of the BCR, binding all the internal controllers and internal processors.

2. New Elements: Third-Party Beneficiary Rights

See 1.1. "New Elements" Section in WP256 (p. 3)

Regarding BCR-C, the "New Elements" section of WP256 notes that with regard to transparency, "all data subjects benefitting from third-party beneficiary rights should in particular be provided with information as stipulated in Articles 13 and 14 GDPR and information on their rights in regard to processing and the means to exercise those rights, the clause relating to liability and the clauses relating to the data protection principles". With regard to notice, the WP29 should clarify that the BCR need only include that this is a requirement and not that BCR are used to provide the actual notice with all the elements of Articles 13 and 14 of the GDPR.

Additionally, the WP29 should clarify that the provision of information about rights in regard to processing and the means to exercise those rights, liability clauses and clauses on data protection principles can be provided in flexible/alternative formats such as by a link from the BCR to other privacy notices, privacy policies or other transparency mechanisms.

Recommendation: Clarify the BCR need only include the requirement that individuals benefitting from third-party beneficiary rights be provided with the information as required by Articles 13 and 14 of the GDPR and that the BCR do not need to restate the actual notice elements of these provisions. In addition, clarify that information on third-party beneficiary rights, liability clauses and data protection principles may be provided in flexible/alternative formats (e.g. links to privacy notices, policies or other transparency mechanisms).

Comments Applicable to Processor BCR Only (BCR-P)

This section of comments concerns WP257 only.

1. BCR-P Scope of Application

See 1. "New Elements" Section in WP257 (p. 3)

Regarding BCR-P, under the "New Elements" section of WP257, the WP29 suggests that BCR-P must specify data transfers, categories of personal data, types of processing and its purposes, types of individuals affected, and the recipients in third countries. We note that for most processors, delivering multiple processing activities and services to many clients, in many industry or government verticals, it is impossible to specify such elements in detail in BCR-P. Processors will not be able to specify such information until the moment they enter into an agreement with a specific client. BCR-P are drafted in a general way, and the specifics of each client contract will be different depending on each client and service. These can be best specified in each service level agreement with the controller and not in the BCR-P. Additionally, the processor would maintain this information as part of its record keeping duty under Article 30 GDPR.

<u>Recommendation</u>: Delete the requirement that BCR-P must specify data transfers, categories of personal data, types of processing and its purposes, types of individuals affected, and the recipients in third countries or refer to this requirement being fulfilled by virtue of the service level agreement, and/or records of processing obligations under Article 30 of the GDPR.

2. <u>New Elements: Third-Party Beneficiary Rights</u>

See 1. "New Elements" Section in WP257 (p. 3)

Regarding BCR-P, the "New Elements" section of WP257 lists third-party beneficiary rights, the right to lodge a complaint and data protection principles. These rights and obligations, however, are limited in respect of processors, because unlike controllers who have to comply with the full set of GDPR requirements, processors have only certain direct statutory obligations under the GDPR. For example, BCR-P cannot specify compliance obligations with principles of fairness, lawful processing and transparency, when these obligations apply only in respect of controllers and not processors. Equally, individuals, de facto, can only lodge a complaint against processors in respect of their direct obligations under the GDPR, such as data security or data transfers, but not in respect of substantive data protection principles, such as grounds for processing or fair processing requirements. The same applies to third-party beneficiary rights.

<u>Recommendation</u>: The WP29 should clarify in the "New Elements" section of WP257 that these elements apply only in respect of direct statutory obligations for processors under the GDPR, such as data security, appointing a DPO, data transfers, use of sub-processors, etc. (many of these are enumerated in Section 1.3 of the main table).

3. <u>Creation of Third-Party Beneficiary Rights for Individuals</u>

See Section 1.3 of Table in WP257 (p. 5-8)

For BCR-P, Section 1.3 of WP257 notes that the individual must be able to enforce the duty of the processor to cooperate with and assist the controller in complying/demonstrating compliance with the law such as for answering requests from data subjects in relation to their rights. CIPL believes the WP29 should place emphasis on the example and further reiterate that the ability to enforce such a duty by the individual should be limited to the situations where the processor BCR entity is not cooperating with the controller to allow for the exercise of the individual's rights or their right to make a complaint. It should not apply to enforcing the general duty to cooperate with the controller, which is the prerogative of the controller and not the individual.

<u>Recommendation</u>: Emphasise that an individual's ability to enforce the processor's duty to cooperate with and assist the controller in complying and demonstrating compliance with

the law is limited to situations where the cooperation is required to allow the individual to exercise their rights or make a complaint.

4. Existence of an Audit Program Covering the BCR

See Section 2.3 of Table in WP257 (p. 11)

For BCR-P, Section 2.3 of WP257 notes that any processor or sub-processor processing the personal data on behalf of a particular controller will accept, at the request of that controller, to submit their data processing facilities for audit of the processing activities relating to that controller. Such audit shall be carried out by the controller or an inspection body composed of independent members and in possession of the required professional qualifications, bound by a duty of confidentiality, selected by the data controller, where applicable, in agreement with the Supervisory Authority.

The requirement to submit data processing facilities for auditing of processing activities is not consistent with Section 6.1.2 or Article 28(3)(h) of the GDPR which require that the processor make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. In practice, it is difficult for most organisations serving multiple clients to allow physical or virtual access and audit to facilities. This is a well-recognised and understood point in commercial discussions and IT service contracts. Furthermore, in practice, sub-processors are very unlikely to accept such an intrusive requirement, especially in cloud services and where doing so may infringe upon the duty of confidentiality of the sub-processor towards its other customers-controllers. While some processors may have less commercial concerns with controllers' access to their facilities, it is still important to limit this access so as not to overwhelm the processors who are serving multiple controllers.

Therefore, CIPL recommends that the WP29 clarify that the completion of questionnaires or provision of independent audit reports conducted by third-party qualified auditors is sufficient to meet the requirement that the processor/sub-processor demonstrate compliance under Article 28(3)(h) of the GDPR. Additionally, BCR-P should allow for certifications to be used in accordance with Article 28(5) in lieu of opening facilities for audit. When an appropriate certification provided by a recognised body under Article 42 exists, this would be sufficient to satisfy the processor's obligations under Article 28(3)(h).

Recommendation: Delete the requirement that processors must open their data processing facilities for auditing of processing activities and clarify that the completion of questionnaires or provision of independent audit reports conducted by third-party qualified auditors is sufficient to meet the requirements of Article 28(3)(h) of the GDPR. Additionally, clarify that certifications can be used in accordance with Article 28(5) GDPR to demonstrate, by processor BCR entities, compliance with Article 28(3)(h) of the GDPR.

5. Rules on Onward Transfers to External Sub-Processors

See Section 6.1 of Table in WP257 (p. 18)

For BCR-P, WP257 notes that "data may [be] sub processed by non-members of the BCR only with the prior informed specific or general written authorization of the controller". A footnote details that this includes information on the main elements (parties, countries, security, guarantees in case of international transfers, with a possibility to get a copy of the contracts used). This is an unrealistic requirement. In practice, processors and sub-processors are likely to refuse to provide copies of their agreements for confidentiality reasons. Additionally, providing a copy of the contracts used is not required for any other mechanisms for data transfers — i.e. adequacy decisions or EU model clauses. This should therefore not be required for transfers based on BCR.

Recommendation: In the case of onward transfers to external sub-processors, delete the requirement to provide a copy of the contracts used as many processors and sub-processors are likely to refuse such a requirement, which will render the BCR unusable.

6. BCR-P Commitments to be Taken in the Service Level Agreement

See Part II "*Commitments to be Taken in the Service Level Agreement" in *WP257 (p. 21)

For BCR-P, WP257 outlines certain required elements to be included in the service level agreement provided by Article 28 of the GDPR. CIPL believes that some of these go beyond the requirements of Article 28 and are extremely difficult for companies to implement in practice and not commercially viable. As a principle, given the very complex commercial negotiations involved in finalising service agreements, we do not believe that commercial contractual terms should be determined by regulators, beyond the legal requirements of the GDPR. At best, regulators should provide more generic guidance and the objectives to be achieved, leaving it to companies and commercial lawyers to negotiate and specify the right approach, based on legal and commercial considerations.

(i) **"BCR will be made binding through a specific reference to it in the [service level agreement]."** The BCR are already binding for processors (based on their own internal binding nature) and they don't need to be binding for controllers. Rather than be made binding, BCR need to be referenced in the service agreement as governing the processing of personal data which are the subject of, or for the purpose of delivering and complying with, the agreement. At a maximum, the processor should agree and warrant that they have valid and approved BCR in place.

(ii) **"The Controller shall commit that if the transfer involves special categories of data the Data Subject has been informed or will be informed before the transfer that his data could be transmitted to a third country not providing adequate protection."** This requirement is excessive, as the transfer is being made to a processor who is not allowed (contractually or legally) to process data for another purpose or use data outside of the instructions provided

by the controller. Furthermore, this requirement is not a requirement of Article 28 of the GDPR and the controller is already required to provide notice about data transfers under Article 13 of the GDPR.

(iii) **"The Controller shall also commit to inform the data subject about the existence of processors based outside of [the] EU and of the BCR. The Controller shall make available to the Data Subjects upon request a copy of the BCR and of the service agreement (without any sensitive and confidential commercial information)."** It is difficult to see how a copy of the BCR-P can be provided to an individual as a single document, given that BCR consist of multiple documents, agreements, policies, procedures and operational documents. Furthermore, providing a copy of the agreement to an individual is commercially unviable, even if all the commercial and confidential information is redacted. Finally, this requirement would impose a burden that no company can address as there could be hundreds and even thousands of processors and sub-processors involved in respect of processing of personal data.

(iv) **"The service agreement will precise [sic][10] if data may be sub-processed inside of the [g]roup or outside of the group and will precise [sic][11] if the prior authorisation to it expressed by the controller is general or needs to be given specifically for each new sub-processing activities."**

CIPL believes that although these obligations apply generally, the WP29 should either remove or make optional the requirement to expressly reference these provisions in the service level agreement. Not only do these requirements go beyond what is required by Article 28 of the GDPR but most companies have also undergone considerable efforts to update all existing agreements with their controllers and processors. Adding these requirements would mean a new marathon of updating agreements four months before the GDPR enters into force, which is entirely unrealistic.

Furthermore, imposing additional obligations on controllers, in the service level agreement, may disincentive their use of BCR-approved processors which could lead to the BCR being viewed as an unusable mechanism by both controllers and processors.

<u>Recommendation</u>: Amend or remove as appropriate the requirement to include the points above in the service level agreement for BCR-P. Work with industry to set desired objectives and outcomes of the service level agreement, rather than prescribing specific terms it should include.

[10] This wording appeared in WP257. We assume that the intended meaning was the service agreement will "specify".
[11] Ibid.

General Comments

1. Evolving the BCR as a Transfer Mechanism

In addition to updating the Working Documents on BCR to reflect the updates introduced by the GDPR, the WP29 also updated its Adequacy Referential[12] which details assessing levels of data protection in third countries and international organisations for purposes of obtaining a finding of adequacy. The Referential notes that core data protection principles have to be present in a third country's legal framework or international organisation in order to ensure essential equivalence with the EU framework. CIPL notes that the core data protection principles outlined in Chapter 3 of the Referential completely align with and map to the principles to be included in BCR. The following table outlines this overlap:

Adequacy Referential General Data Protection Principles – Chapter 3 Adequacy Referential	**BCR Key Principles WP256 (6.1.1, p. 16) and WP257 (6.1, p. 15)**
Concepts	Utilises GDPR Terminology
Grounds for Lawful and Fair Processing for Legitimate Purposes	Transparency, Fairness and Lawfulness
The Purpose Limitation Principle	Purpose Limitation
The Data Quality and Proportionality Principle	Data Minimisation and Accuracy/Data Quality
Data Retention Principle	Limited Storage Periods
The Security and Confidentiality Principle	Security
The Transparency Principle	Transparency, Fairness and Lawfulness
The Right of Access, Rectification, Erasure and Objection	Data Subject Rights
Restriction on Onward Transfers	Restrictions on Transfers and Onward Transfers

The inclusion of BCR principles identical to those required for a finding of adequacy strongly supports the view that having an approved BCR presumes that a multinational company has a uniform and "adequate" level of data protection within the group which enables the entities to process, transfer and share data freely within the group (but always in compliance with BCR and underlying GDPR requirements). This is similar to, although not legally the same as, the "adequacy" finding at the country level. Thus, CIPL believes that any data transfers to and processing of data by a BCR-approved company (from another company) and between BCR-approved companies should be permitted without any additional transfer mechanism (model clauses or derogations, for example).

Furthermore, if transfers from the EU to a US-based Privacy Shield-certified company can take place based on self-certification with Privacy Shield, then transfers from the EU to a BCR-approved company should also be allowed.

Therefore, CIPL believes that there are strong policy and practical arguments that support the evolving of BCR into a more universal and usable mechanism that can frame many modern data transfers. CIPL suggests that the WP29 clarify that international transfers

[12] WP254 Adequacy Referential (updated) http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48827.

should be permitted to take place (without additional transfer mechanisms such as model clauses or derogations in place):

a) between two BCR-approved companies (either controllers or processors), as both companies will have high levels of privacy protection within their groups in respect of all the data they receive and share. This would mean that specifically controller to controller and processor to sub-processor transfers should be permitted.

b) from any controller (not BCR-approved) to a BCR-approved controller. This makes sense given that a controller today can transfer data to a processor outside its group if that processor has BCR in place.

Additionally, the GDPR expands the application of BCR from use within a corporate group to a group of enterprises "engaged in a joint economic activity". The GDPR does not define the meaning of "engaged in a joint economic activity". CIPL believes this term could be interpreted broadly to cover the scenarios mentioned above where two groups of companies engage in a formal or commercial and contractual relationship in respect of a provision of a service, development of a product or a joined collaboration or activity which involves some data sharing between two organisations.

Given the deep experience of building and implementing BCR within CIPL and some of its members, CIPL will continue to work with interested and accountable organisations and DPAs, the WP29/EDPB and the Commission in exploring these options and how they may work in practice with the changes brought by the GDPR.

Recommendation: Clarify that BCR companies are adequate companies and therefore transfers between two BCR-approved companies (either controllers or processors) or transfers from any controller (not BCR-approved) to a BCR-approved controller are permitted. Clarify the meaning and examples of companies "engaged in a joint economic activity" as suggested above.

2. BCR and Brexit

In light of Brexit, we invite the WP29 to consider the application of BCR post-Brexit, and under the assumption that BCR will also exist as a mechanism under the new UK data protection law. BCR, approved by the ICO as lead authority (and agreed by the other DPAs in the application), should continue to be recognised beyond that date and the WP29 should further consider the ongoing role of the UK Information Commissioner's Office (ICO) as a lead DPA for approved BCR post-Brexit. Furthermore, BCR-approved entities who have chosen to relocate their operations and split their group headquarters to more than one EU country as a result of Brexit should be able to choose a single EU lead Supervisory Authority for the split group headquarters, operating under the same BCR, as the division is based on operational reasons rather than any substantive change in the original BCR itself.

<u>Recommendation</u>: Clarify the status for existing and UK approved BCR post-Brexit, the future role of the UK ICO surrounding the BCR and the situation for new BCR applications post-Brexit. Additionally, the WP29 should clarify that a corporate group headquarters, split among different EU Member States for operational reasons post-Brexit should be able to appoint a single EU lead Supervisory Authority for the split group headquarters.

3. <u>BCR Interoperability</u>

In line with interest expressed by the Commission on exploring ways to promote convergence between BCR under EU law and the CBPR as regards applicable standards and application processes under each system,[13] the WP29 should recommend the Commission consider possible interoperability between BCR and other transfer mechanisms (e.g. APEC CBPR, GDPR Certifications, etc.) and promote such interoperability through appropriate means and processes.[14]

<u>Recommendation</u>: Highlight the importance of BCR interoperability with other transfer mechanisms and propose the Commission consider and promote such interoperability through appropriate means and processes.

4. <u>Streamlining the BCR Process</u>

The comments above demonstrate the importance of streamlining the BCR documentation requirements to ensure BCR uptake by many companies. CIPL believes that the review and approval process should also be streamlined further and perhaps changed substantially. Ideally and in the long run, BCR should not require prior approval by DPAs as it is currently understood. Instead, BCR should be based on a review by a third-party (an accredited certification body under the GDPR, or an "Accountability Agent" as in the APEC CBPR system) or, going a step further, on a self-certification system (like the Privacy Shield). Indeed, a third-party review system could be devised that fully meets the DPA approval requirement in Article 47(1) of the GDPR. Augmenting the BCR process with such a third-party review process would ease the current burden on DPA resources for approving BCR and facilitate faster BCR processing times for both companies and regulators. Nevertheless, for the time being, Article 47(1) is interpreted to mean that BCR be approved by a competent authority directly and without the assistance of a third-party Accountability Agent. Therefore, until such a time as such a third-party review (or even self-certification) system can be developed to meet the requirements of Article 47(1), all efforts should be

[13] Communication from the Commission to the European Parliament and the Council; Exchanging and Protecting Personal Data in a Globalised World, Brussels 10.1.2017, COM (2017) 7 final, at page 11 http://ec.europa.eu/newsroom/document.cfm?doc_id=41157.
[14] See CIPL White Paper in Footnote 3 at page 12 for further discussion.

made to ensure that the BCR review, approval and documentation process is made as scalable, affordable and accessible as possible under present conditions.

Recommendation: Streamline the BCR documentation requirements through adopting the recommendations made throughout this document. Recommend that the Commission consider third-party BCR approval by approved certification bodies or "Accountability Agents" and/or a self-certification system for BCR which would streamline the whole BCR approval process and facilitate faster processing times.

Conclusion

CIPL is grateful for the opportunity to provide comments on key implementation questions regarding Binding Corporate Rules. We look forward to providing further input on BCR in the future as new issues arise, particularly in light of any practical experiences in applying the GDPR.

If you would like to discuss any of these comments or require additional information, please contact Bojana Bellamy, bbellamy@hunton.com, Markus Heyder, mheyder@hunton.com or Sam Grogan, sgrogan@hunton.com.